

ISPConfig nginx Logfiles an Graylog-Server schicken

Diese Konfiguration schickt nginx Access- und Errorlogs über GELF an einen Graylog-Server. Der GELF-Input im Graylog sollte natürlich aktiviert sein. Das Pattern-Matching funktioniert leider noch nicht exakt.

/etc/logstash/patterns.d/nginx-access.conf

```
NGINX_WEBSITE /[^\s]+/[^\s]+/[^\s]+/[^\s]+/(?<website>[^\s]+)/
```

/etc/logstash/patterns.d/nginx-error.conf

```
HTTPERRORDATE %{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{YEAR}  
NGINXERRORLOG \[%{HTTPERRORDATE:timestamp}\] \[%{WORD:severity}\] \[client %{IPORHOST:clientip}\]
```

/etc/logstash/conf.d/nginx.conf

```
# nginx log input  
input {  
  file {  
    type => "nginx-access"  
    path => ["/var/log/ispconfig/httpd/*/access.log"]  
  }  
  file {  
    type => "nginx-error"  
    path => ["/var/log/ispconfig/httpd/*/error.log"]  
  }  
}  
  
# filters  
filter {  
  if [type] == "nginx-access" {  
    grok {  
      match => { "message" => "%{COMBINEDAPACHELOG}" }  
    }  
    grok {  
      patterns_dir => ["/etc/logstash/patterns.d"]  
      match => [ "path", "%{NGINX_WEBSITE}" ]  
    }  
  }  
  
  if [type] == "nginx-error" {  
    grok {  
      match => { "message" => "%{NGINXERRORLOG}" }  
      patterns_dir => ["/etc/logstash/patterns.d"]  
    }  
  }  
  
  if !("_grokparsefailure" in [tags]) {  
    mutate {  
      remove_field => [ "message" ]  
      add_field => [ "timestamp_submitted", "%{@timestamp}" ]  
    }  
  
    date {  
      match => [ "timestamp", "EEE MMM dd HH:mm:ss yyyy" ]  
      remove_field => [ "timestamp" ]  
    }  
  
    geoip {  
      source => "clientip"  
    }  
  }  
}
```

```
}  
  
# output  
output {  
  #stdout {  
    # #codec => "plain"  
    # codec => "rubydebug"  
  }  
  gelf {  
    host => "log.myserver.de"  
    port => 12201  
  }  
}
```

Revision #1

Created 30 April 2021 12:16:26 by magenbrot

Updated 30 April 2021 12:16:55 by magenbrot